Statement of Mr. David J. McIntyre, Jr.
President and CEO
TriWest Healthcare Alliance
Before the House Veterans' Affairs Committee
Subcommittees on Oversight and Investigations
and Technology Modernization
December 14, 2022

Introduction

Chairman Pappas, Chairman Mrvan, Ranking Member Mann, Ranking Member Rosendale and Distinguished Members of the Subcommittees, thank you for the opportunity to share the efforts TriWest Healthcare Alliance undertakes to ensure the security of the Veteran data we are entrusted to use in fulfilling our role in support of VA community care. Cyberattacks and data breaches are not only growing more sophisticated but incidents continue to increase year over year. Remaining focused and vigilant is critical. We commend you for holding this hearing on this very important matter.

Established over 25 years ago by a group of non-profit Blue Cross Blue Shield plans and two university hospital systems, TriWest Healthcare Alliance has been honored to have as our sole mission supporting the Department of Veterans Affairs (VA) and Department of Defense (DoD) in meeting the health care needs of the military and veteran communities. Since inception, we at TriWest have worked collaboratively with the federal government agencies we have been privileged to support to fully understand their unique needs, down to the local level, to meet the health care needs of military service members, their families, retirees and Veterans. Our mission has been, and continues to be, doing "Whatever it Takes" to ensure our Nation's heroes and their families have ready access to needed care when the federal systems on which they rely are unable to meet their needs directly. And, our network just surpassed the staggering milestone of delivering more than 50 million total appointments – in every category of care – in support of VA's mission to provide for the needs of those who borne the battle... Strengthening VA and its ability to keep faith with our nation's finest.

Our first 18 years were spent supporting DoD in standing up and operating the TRICARE program in a 21-state area. I am proud of the work that we did to assist DoD in implementing and refining TRICARE to meet the needs of millions of TRICARE beneficiaries across the TRICARE West Region who relied on us for services and support. However, it was not an easy or painless road. In addition to the many challenges we and the Department of Defense encountered standing up a new program, challenges similar to those experienced with other new large health programs, we also had the opportunity to learn far more about data security threats and the need for all of us – state, federal and local government, private sector organizations and individuals – to be ever vigilant and to pursue all appropriate security protection measures. But, even when you have done so, you can find yourself compromised due to the actions of others.

In December 2002, thieves broke into one of our offices and stole hard drives containing the personal data of over 500,000 customers – members of the military, retired military and their

families. We had but one question on our mind. How did we keep information theft from morphing into identity theft and bringing harm to those we were entrusted to serve? I was told that we had seven days to inform our customers of what had happened and how they could go about placing a fraud flag on their credit file. It necessitated undertaking a massive communications campaign to try and reach everyone affected, regardless of where they were located for the holidays. We contacted all of the major media across the country, including all broadcast networks, and built a massive call center to handle phone calls and asked our staff to work around the clock and through the holiday period. We also offered a $100,000 reward to assist authorities in the attempt to apprehend the thieves. In addition, we built a special website and literally sent out millions of letters regarding the theft. I am pleased to report that based on our rapid response to this terrible event, none of the individuals whose personal information was contained in these hard drives ended up being harmed by this theft!

One key lesson we learned was that, at the time, the laws to protect consumers and how credit bureaus treated customers had become antiquated. So we proactively brought our experience here, to Capitol Hill, and worked with Congress and the Administration to change all of that. As a result of those joint efforts, amendments to the Fair Credit Reporting Act were enacted that provided a broad suite of enhanced protections for consumers, including an annual credit report for free and the ability of a company to file fraud flags for the their customers who are at risk due such an event.

The experience also helped our employees understand our ethical framework – putting the customer first rather than the corporation… Doing whatever it takes! And, while this theft occurred 20 years ago, it still guides our approach today. We take protecting data security very, very seriously and incorporate substantial protective measures to protect the personal data of every Veteran we serve. After all, we are merely the custodian for their personal information.

VA Requirements

Our Business Associate Agreement (BAA) with VA requires us to protect Veterans personal health information (PHI) to the greatest extent feasible in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("HIPAA Rules"), 45 C.F.R. Parts 160 and 164, for the Use and Disclosure of Protected Health Information (PHI) under the terms and conditions specified in our business agreement with VA.

These terms and conditions require implementing appropriate administrative, physical, and technical safeguards and controls to protect PHI and document applicable policies and procedures to prevent any unauthorized use or disclosure of PHI. We also are required to notify VA no later than by midnight following the next business day after discovery of any incident and provide a written report to VA of any potential access, acquisition, use, disclosure, modification, or destruction of either secured or unsecured PHI in violation of the BAA, including any incident or breach of PHI, within ten (10) business days of the initial notification to VA.

Protection/Prevention

As discussed earlier in this testimony, we have drawn upon our data theft experience of 20 years ago to implement very stringent administrative, physical and technical safeguards and controls to protect PHI. These measures have been enhanced over the years as technology has advanced, and we continue to remain focused on doing whatever it takes to ensure the security of Veteran personally identifiable information and PHI. TriWest diligently monitors our networks and solutions and makes continuous improvements to ensure a high detection and prevention rate in protecting our Nation's Veterans information. Some of the current measures we have in place include:

Administrative

1. First and foremost, we flow all BAA data security requirements down to our subcontracted partners who may have any opportunity to encounter Veteran PHI.

2. We have an appointed HIPAA Privacy Official who oversees HIPAA Privacy Rules and guidelines and is charged with ensuring full compliance of HIPAA across the organization.

3. All TriWest staff are required to take several training courses that focus on various aspects of information security:
    a. Information Security Awareness (Required Annually): This training increases awareness and knowledge of information security and for employees to know how to respond to information security threats, should they ever occur.
    b. Utilization Review Accreditation Commission (URAC) (Required Annually): This module provides our employees with an understanding of URAC, URAC Core Standards, and how TriWest maintains URAC Accreditation ensuring our adherence to quality standards and commitment to continuous improvement.
    c. HIPAA for New Employees: This course provides knowledge of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Upon completion of this course, individuals will have an understanding of the HIPAA Privacy and Security rules, will be able to identify the administrative, physical, and technical safeguards TriWest implements to comply with HIPAA, will be able to apply the HIPAA Privacy Security rules to their job function, and report a breach.
    d. HIPAA Refresher (Required Annually): This training assesses our employees continued understanding of the information learned in the HIPAA for New Employees module
    e. Federal Statutes: This course introduces staff to the federal statutes that apply to TriWest's work.
    f. Sensitive Diagnosis: This module teaches about specific diagnoses that have special, extra protections over and above HIPAA.

Physical

Physical safeguard includes providing TriWest employees an identification badge to access TriWest buildings and facilities, limiting building entry outside work hours, requiring visitors to sign-in with building security.

Technical

TriWest takes a "Defense in Depth" approach to securing our Nation's Veteran information and meeting our security requirements. We apply multiple solutions and processes that work together in a layered methodology to help prepare, prevent, detect, analyze, contain, eradicate and recover from an ever changing threat landscape. These tools and processes include, among other things, using and applying:

1. An always available, 24/7/365 Security Operation Center (SOC), in partnership with IBM, that monitors TriWest's entire IT infrastructure, 24x7, to detect cyber events in real time and proceed to address them immediately. This team of Security professionals selects, operates, maintains the cybersecurity technologies, and continually analyzes event and threat data to find ways to improve TriWest's security posture. This function continuously works to improve preventative measures and security policies, create faster event and threat detection, and provide more efficient and more cost effective response to cyber events and threats, thus providing the on-going processes in reducing TriWest's overall risk profile and increase system reliability. For example, TriWest Security and SOC teams incorporate threat Intelligence feeds from the U.S. government and private industry and keeping up with new and trending attacks and ensuring that security systems have an updated set of rules to help detect such attacks. They also continuously identify, apply, and test mitigation steps and or patches for vulnerable enterprise systems and software.

2. Federal Security Framework that follows the six-step National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) Security Assessment & Authorization (SA&A) approach, to categorize, select, implement controls, assess, authorize, and monitor risks. TriWest delivers our services by collaborating with all stakeholders, facilitating, and coordinating communications throughout all steps of the system authorization workflow. Our approach not only satisfies FISMA requirements but also enables continued security as threats and business needs evolve.

3. Ingress/Egress Security (IES) using technology, techniques, and processes in order to identify, prevent, report and respond to cyber events and threats from external systems, networks and people. It also provides this same functionality for traffic leaving TriWest's network boundary.

4. Network Data Loss Prevention (NDLP) that identifies the content within specific network traffic and prevents that content from leaving a network boundary, thus protecting the confidentiality of TriWest's sensitive data. This service integrates with SOC service, and handles both encrypted and non-encrypted network traffic.

5. Vulnerability Management with ongoing, regular process of identifying, assessing, reporting on, managing and remediating cyber vulnerabilities within the TriWest combined service environment. This service integrate the Vulnerability Assessment information with SOC service to assist in more accurate threat detection.

6. Incident Response plan that includes requirements identified within the NIST 800-61 Rev2, Computer Incident Handling Guide which define four phases of incident handling – Preparation, Detection & Analysis, Containment, Eradication & Recovery, and Post-Incident Activity. The plan includes details around all four phases including pre-defined playbooks for various scenarios, process flows, points of contact, and organizational structure.

7. Internal policies and procedures to protect electronic PHI (ePHI) such as requiring unique user account logins and passwords to access ePHI, and continually assessing internal software applications that store ePHI for vulnerabilities and appropriate security controls.

Action/Response to Security Issues

TriWest has clearly defined policies and procedure for addressing any possible data security violation, and as mentioned in our prevention section, trains all employees on how to report any possible data security incident.

In the event a TriWest employee discovers a possible data breach, it is immediately reported to the TriWest HIPAA Privacy Official. With the available information, the HIPAA Privacy Official conducts a Risk Assessment using an assessment obtained from the Department of Health and Human Services. If the reported incident is confirmed to be a breach or possible breach, the HIPAA Privacy Official notifies the VA as directed in our BAA with VA, within 24 hours. We then provide all relevant information surrounding the incident and identify the information involved within 10 business days, and submit a final Security Incident Investigation Report.

VA's BAA is appropriately very stringent. In comparison, HIPPA requires notifying HHS of a breach affecting 500 or more individuals to be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach. If a breach affects fewer than 500 individuals, the notification may be done on an annual basis but no later than 60 days after the end of the calendar year in which the breach is discovered. Under the VA BAA, we report even a single incident within 24 hours.

Reported Incidents

TriWest has not had any system security breaches in the last 5 years. We have, however, experienced a few major national incidents that initiated our incident response processes to investigate possible compromise, such as the Log4j – Apache Software Vulnerability (November 2021) and Solarwinds Software hack (December 2020). In each of these incidents, TriWest responded and performed a full scale and company-wide incident response and analysis that determined the incidents were benign within our networks.

In addition to investigating possible compromise as a result of these national incidents, we have had a very small number of individual privacy and/or security incidents since the start of our Community Care Network contracts. In 2020, we submitted 2 breach notifications to VA; in 2021 we submitted 3, but later confirmed there was no breach in one of the 3 submitted; and in 2022 to date, we have provided no notifications to VA.

The types of privacy incidents these notifications represent include an Explanation of Benefits (EOB) sent to an incorrect Veteran or an authorization sent to an incorrect provider. In the case of the EOB sent to a different Veteran, no breach occurred because the incorrect information on the EOB is the date of service, procedure and payment amount, but not the name, address or SSN of the correct Veteran. Therefore, there is nothing to tie the information sent to the incorrect Veteran to the correct Veteran. Authorizations sent to incorrect providers occur when the appointment letter and consult are sent, typically by fax, to an incorrect provider. Since the incorrect provider is a Covered Entity according to HIPAA rules, they are required to notify TriWest of the errors, destroy the information and cannot further disclose it. Therefore there is no risk to the Veteran, and this would not be a breach.

Closing

In closing, Chairman Pappas, Chairman Mrvan, Ranking Member Mann and Ranking Member Rosendale, I would again like to thank you for addressing this very important topic. I hope that my testimony fully conveys the deep commitment TriWest Healthcare Alliance has to doing our level best to protect the personal information of those we are entrusted to serve… our nation's heroes. We unfortunately learned firsthand of the extent that bad actors will go to steal valuable data and the need for all of us to be ever vigilant. Working together with law enforcement, Congress and the Federal Government, we used our experience of 20 years ago to set standards for protecting consumers when data security crimes and breaches occur. Our experience proved that a timely, full-scale response is the best approach to ensuring we protect those whose personal information might be compromised. We all need to be ready to do Whatever it Takes if we find ourselves compromised to ensure the security of our Veterans' personal information, as well as their personal health and wellness. They deserve nothing less!